

Period Distribution of Inversive Pseudorandom Number Generators Over Finite Fields

Bo Zhou^{1,*}, Qiankun Song²

¹College of Information Science & Engineering, Chongqing Jiaotong University, Chongqing 400074, P.R. China

²Department of Mathematics, Chongqing Jiaotong University, Chongqing 400074, P.R. China

Abstract

In this paper, we focus on analyzing the period distribution of the inversive pseudorandom number generators (IPRNGs) over finite field $(\mathbb{Z}_N, +, \times)$, where $N > 3$ is a prime. The sequences generated by the IPRNGs are transformed to 2-dimensional linear feedback shift register (LFSR) sequences. By employing the generating function method and the finite field theory, the period distribution is obtained analytically. The analysis process also indicates how to choose the parameters and the initial values such that the IPRNGs fit specific periods. The analysis results show that there are many small periods if N is not chosen properly. The experimental examples show the effectiveness of the theoretical analysis.

Keywords: Inversive pseudorandom number generators (IPRNG); Linear feedback shift register (LFSR); Period distribution; Finite field.

I. INTRODUCTION

Pseudorandom number generators (PRNGs) are deterministic algorithm that produces a long sequence of numbers that appear random and indistinguishable from a stream of random numbers [1], which are widely employed in science and engineering, such as Monte Carlo simulations, computer games and cryptography. In recent years, a variety of PRNGs based on nonlinear congruential method [2], [3], chaotic maps [4]–[6] and linear feedback shift registers (LFSRs) [7], [8] are proposed. These PRNGs are implemented on finite state machines, which lead to the fact that sequence generated by them are ultimately periodic. In cryptographic applications, a long period is often required. Once the period is not long enough, the encryption algorithms may be vulnerable to attacks, e.g., in [7], Kocarev *et al.* proposed a public key encryption algorithms based on Chebyshev polynomials over the finite field, but in [9], [10], Chen *et al.* showed that if the period of the sequence generated by the Chebyshev polynomials is not sufficiently long, the public key encryption algorithm is easy to be decrypted. Therefore, it is worth to making clear that what are the possible periods of a PRNG and how to choose suitable control parameters and initial values such that the PRNG fits specific period, these knowledge helps in algorithm design and its related applications.

In [9], [10], Chen *et al.* analyzed the period distribution of the sequence generated by the Chebyshev polynomials over finite fields and integer rings, respectively, by employing the generating function method. In [11], Chen *et al.* analyzed the period distribution of the generalized discrete Arnold cat map over Galois rings by employing the

* Corresponding author.

E-mail addresses: zhouboqcncq@163.com (B. Zhou), qiankunsong@163.com (Q. Song)

generating function method and the Hensel lifting method. In [12], Chen *et al.* summarized their works on the period distribution of the sequence generated by the linear maps.

In [13], Chou described all possible period lengths of IPRNG (1) and showed that these period lengths are related to the periods of some polynomials. However, the author did not give the full information on period distribution, this leads to the limitation of the applications of IPRNGs. In [14], Solé *et al.* proposed an open problem of arithmetic interest to study the period of the IPRNGs and to give conditions bearing on a, b to achieve maximal period. Although their considered state space is a Galois ring, it is also significant to study this problem in finite field. Recent results on the distribution property in parts of the period of this generator over finite fields can be found in [15], [16] and it would be interesting to generalize these results to arbitrary parts of the period. If the full information on the period distribution is known, we could do such a work.

Motivated by the above discussions, we focus on analyzing the period distribution of the IPRNGs over the finite field $(\mathbb{Z}_N, +, \times)$, where $N > 3$ is a prime. The analysis process is that, first, to make exact statistics on the periods of model (1), then count the number of IPRNGs for each specific period when a, b and x_0 traverse all elements in \mathbb{Z}_N . The sequences generated by model (1) are transformed to 2-dimensional LFSR sequences which is the foundation of the stream ciphers [17]. Then, the detailed period distribution of IPRNGs is obtained by employing the generating function method and the finite field theory. The analysis process also indicates how to choose the parameters and the initial values such that the IPRNGs fit specific periods.

This paper is organized as follows. To make this paper self-contained, Section II presents some preliminaries that help to understand our analysis. In Section III, detailed analysis of the period distribution of the sequences generated by IPRNGs with $ab = 0$ in \mathbb{Z}_N and $x_0 \in \mathbb{Z}_N$. Then Section IV presents the detailed analysis of the period distribution of the sequences generated by IPRNGs with $a \in \mathbb{Z}_N^\times, b \in \mathbb{Z}_N^\times$ and $x_0 \in \mathbb{Z}_N$. Finally, conclusion and some suggestions for future work are made in Section V.

II. PRELIMINARIES

In this section, we introduce relevant notation and definition to facilitate the presentation of main results in the ensuing sections. For the knowledge of finite fields, please refer to [18].

A. Recurring relation over the finite field

Let \mathbb{Z}_N be the residue ring of integers modulo N . When N is prime, $(\mathbb{Z}_N, +, \times)$ forms a finite field to which the modular operation is required in addition and multiplication.

Definition 1: [18]. A sequence a_0, a_1, \dots satisfying the relation over $(\mathbb{Z}_N, +, \times)$:

$$a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \dots + c_k a_n \pmod{N}, \quad (1)$$

where $c_i \in \mathbb{Z}_N$ for all $i = 1, 2, \dots$, is called a linear recurring sequence in \mathbb{Z}_N .

The generation of the linear recurring sequences can be implemented on a linear feedback shift register which is a special kind of electronic switching circuit handling information in the form of elements in \mathbb{Z}_N .

Definition 2: [18]. $f(t) = t^k - c_1 t^{k-1} - \dots - c_k$ is called the characteristic polynomial of recurring relation (1). Also, the sequence a_0, a_1, \dots is called the sequence generated by $f(t)$ in \mathbb{Z}_N .

The characteristic polynomial $f(t)$ plays an important role in analyzing the period of the sequence generated by recurring relation (1). It follows from [10] that if all roots of $f(t)$ are with multiplicity 1, then the period T of a_0, a_1, \dots equals to $\text{per}(f)$. $\text{per}(f)$ is the smallest integer such that $f(t) \mid t^{\text{per}(f)} - 1$, which is called the period of $f(t)$. Then, we have the following proposition on $\text{per}(f)$.

Proposition 1: If $f(t)$ can be factorized as $f(t) = (t - \alpha_1)(t - \alpha_2) \dots (t - \alpha_m)$, where $\alpha_i \neq \alpha_j$ for all $1 \leq i, j \leq m$ and $i \neq j$, then $\text{per}(f) = \text{lcm}(\text{ord}(\alpha_1), \text{ord}(\alpha_2), \dots, \text{ord}(\alpha_m))$, where $\text{lcm}(\text{ord}(\alpha_1), \text{ord}(\alpha_2), \dots, \text{ord}(\alpha_m))$ is the least common multiple of $\text{ord}(\alpha_1), \text{ord}(\alpha_2), \dots, \text{ord}(\alpha_m)$.

Proof: Let $L = \text{lcm}(\text{ord}(\alpha_1), \text{ord}(\alpha_2), \dots, \text{ord}(\alpha_m))$. Since $\alpha_i^L - 1 = 0$ for all $i = 1, 2, \dots, m$, it is valid that

$$t - \alpha_i \mid t^L - 1$$

for all $i = 1, 2, \dots, m$. Since $\alpha_i \neq \alpha_j$ for all $1 \leq i, j \leq m$ and $i \neq j$, it is valid that $t - \alpha_i$ and $t - \alpha_j$ are coprime for all i, j . Thus, $(t - \alpha_1)(t - \alpha_2) \dots (t - \alpha_m) \mid t^L - 1$, which means that $f(t) \mid t^L - 1$. By the property of the order, we have $\text{per}(f) = L$. The proof is completed. ■

In [9], [10], Proposition 1 is employed to analyze the period distributions of two linear maps: the Chebyshev map and the generalized discrete cat map, whose characteristic polynomials can be expressed as $f(t) = t^2 + at + 1 \in \mathbb{Z}_N[t]$, where N is an integer. If α and β are roots of $f(t)$, then it must hold that $\alpha\beta = 1$. Thus, $\text{ord}(\alpha) = \text{ord}(\beta)$. By Proposition 1, we have $\text{per}(f) = \text{ord}(\alpha)$, so $T = \text{ord}(\alpha)$. However, if the characteristic polynomial is $f(t) = t^2 + at + b \in \mathbb{Z}_N[t]$, whose roots are α and β , where $b \neq 1$, we can not conclude that $\text{ord}(\alpha) = \text{ord}(\beta)$. In order to analyze the period T , we should analyze $\text{ord}(\alpha)$ and $\text{ord}(\beta)$, respectively. If N is not chosen properly, i.e., both $N - 1$ and $N + 1$ has many divisors, the analysis process is rather complicated. This obstacle prompts us to adopt another approach which will be presented in Section IV.

B. IPRNGs over the finite field

In this paper, we consider the following IPRNG proposed in [2] over $(\mathbb{Z}_N, +, \times)$:

$$x_{n+1} = \begin{cases} ax_n^{-1} + b & x_n \in \mathbb{Z}_N^\times \\ b & x_n = 0 \end{cases}, \quad (2)$$

for all $n \geq 1$, where $N > 3$ is a prime, $a, b \in \mathbb{Z}_N$. The initial value associated with model (2) is given by $x_0 \in \mathbb{Z}_N$.

Hereafter, we denote $S(x_0; a, b)$ as the sequence generated by model (2) starts from x_0 for given a, b . Then, we have the following definition on the period of $S(x_0; a, b)$.

Definition 3: For every initial value $x_0 \in \mathbb{Z}_N$, the smallest integer $L(x_0; a, b)$ such that $x_{n+L(x_0; a, b)} = x_n$ for all $n \geq n_0 \geq 0$ is called the period of the IPRNGs correspond to a, b and x_0 , where n_0 is a nonnegative integer.

Remark 1: It is noteworthy that the sequence generated by the IPRNGs may not be purely periodic, i.e. every period start from x_0 , which is different from the case for the Chebyshev map and the generalized discrete Arnold cat map. Its period depends on not only the control parameters a, b but also the initial value x_0 , this will be illustrated in Section III and Section IV.

Throughout this paper, \mathbb{Z}_N denotes the residue ring of integers modulo N . \mathbb{Z}_N^\times denotes the group of all units in \mathbb{Z}_N . $(\mathbb{Z}_N, +, \times)$ denotes the finite field where addition and multiplication are all modular operations. For $\alpha \in \mathbb{Z}_N$, denote $\text{ord}(\alpha)$ as the order of α in \mathbb{Z}_N . $\text{GF}(N^2)$ denotes a finite field with N^2 elements. $\varphi(n)$, i.e., Eulers totient

function, denotes the number of positive integers which are both less than or equal to the positive integer and coprime with n .

III. PERIOD DISTRIBUTION OF IPRNGs WITH $ab = 0$ IN Z_N AND $x_0 \in Z_N$

When $ab = 0$ in Z_N and $x_0 \in Z_N$, there are $2N^2 - N$ IPRNGs. It would be better if we have an impression on what the period distribution with $ab = 0$ in Z_N and $x_0 \in Z_N$ looks like. Fig. 1 is a plot of the period distribution of IPRNGs (2) with $ab = 0$ in Z_{31} and $x_0 \in Z_{31}$. It can be seen from Fig. 1 that the periods distribute very sparsely, some exist and some do not.

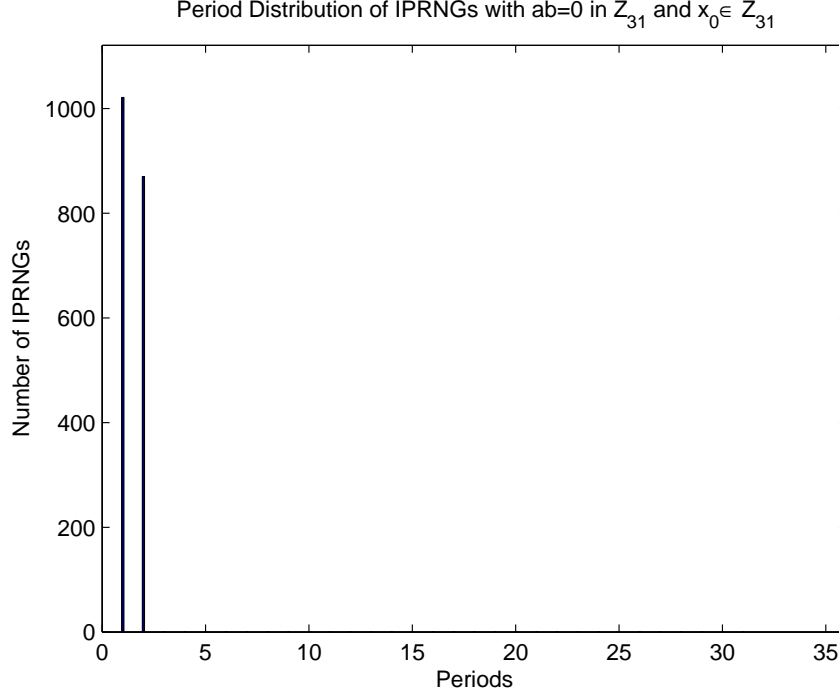


Fig. 1. Period distribution of IPRNGs with $ab = 0$ in Z_{31} and $x_0 \in Z_{31}$.

In [13], Chou has considered the periods of IPRNGs for $ab = 0$ in Z_N and $x_0 \in Z_N$. The results are listed as follows

Proposition 2: Suppose $a = 0$, then $x_n = b$ for all $n \geq 1$ and $L(x_0; 0, b) = 1$.

Proposition 3: Suppose $a \neq 0$ and $b = 0$.

(P1) If $x_0 = 0$, then $x_n = 0$ for all $n \geq 1$ and $L(0; a, b) = 1$.

(P2) If $a = x_0^2$ and $x_0 \neq 0$, then $x_n = x_0$ for all $n \geq 1$ and $L(x_0; x_0^2, b) = 1$.

(P3) If $a \neq x_0^2$ and $x_0 \neq 0$, then $x_{n+2} = x_n$ for all $n \geq 1$ and $L(x_0; a, b) = 2$.

Now, all the possible periods for this case are revealed. In the following, we will count the number of IPRNGs for each specific period and present the period distribution.

Theorem 1: For IPRNG (2) with $ab = 0$ in Z_N and $x_0 \in Z_N$, the possible periods and the number of each special period are given in Table I.

Proof: For $L(x_0; a, b) = 1$, there are three cases:

TABLE I
PERIOD DISTRIBUTION OF IPRNGs WITH $ab = 0$ IN Z_N AND $x_0 \in Z_N$.

Periods	Number of IPRNGs
1	$N^2 + 2N - 2$
2	$(N - 2)(N - 1)$

TABLE II
PERIOD DISTRIBUTION OF IPRNGs WITH $ab = 0$ IN Z_{31} AND $x_0 \in Z_{31}$.

Periods	Number of IPRNGs
1	1021
2	870

(i) $a = 0$. Here, the choice of a is unique and there are N choices of b and N choices of x_0 . Thus, there are N^2 IPRNGs.

(ii) $a \neq 0, b = 0$ and $x_0 = 0$. Here, there are $N - 1$ choices of a and the choices of b and x_0 are unique. Thus, there are $N - 1$ IPRNGs.

(iii) $a \neq 0, b = 0$ and $a = x_0^2$. Here, there is a unique choice of b . Since $a \neq 0$ and $a = x_0^2$, it is valid that $x_0 \neq 0$. Thus, there are $N - 1$ choices of x_0 . Once x_0 is chosen, a is uniquely determined. Thus, there are $N - 1$ IPRNGs.

Combining (i), (ii) and (iii), we have there are $N^2 + 2N - 2$ IPRNGs for $L(x_0; a, b) = 1$.

For $L(x_0; a, b) = 2$, since $x_0 \neq 0$, there are $N - 1$ choices of x_0 . Once x_0 is chosen, combining $a \neq 0$, there are $N - 2$ choices of a and a unique choice of b . Thus, there are $(N - 2)(N - 1)$ IPRNGs. The proof is completed. ■

Example 1: The following example is given to compare experimental and the theoretical results. A computer program has been written to exhaust all possible IPRNGs with $ab = 0$ in Z_{31} and $x_0 \in Z_{31}$ to find the period by brute force, the results are shown in Fig. 1.

Table II lists the complete result we have obtained. It provides the period distribution of the IPRNGs. As it is shown in Fig. 1 and Table II, the theoretical and experimental results fit well. The maximal period is 2 while the minimal period is 1. The analysis process also indicates how to choose the parameters and the initial values such that the IPRNGs fit specific periods.

IV. PERIOD DISTRIBUTION OF IPRNGs WITH $a \in Z_N^\times, b \in Z_N^\times$ AND $x_0 \in Z_N$

In [13], Chou described all possible periods of the model (2) with $a \in Z_N^\times, b \in Z_N^\times$ and $x_0 \in Z_N$ and showed that these periods were related to the periods of several polynomials, see Theorem 2 and Theorem 4 in [13]. However, the author did not provide a feasible way to evaluate these periods. In the following, we will characterize the full information on the period distribution of sequences generated by IPRNG (2) with a, b traverse all elements in Z_N^\times and x_0 traverses all elements in Z_N .

When a, b traverse all elements in Z_N^\times and x_0 traverse all elements in Z_N , there are $(N-1)^2N$ IPRNGs. It would be better if we have an impression on what the period distribution with $a \in Z_N^\times$, $b \in Z_N^\times$ and $x_0 \in Z_N$ looks like. Fig. 2 is a plot of the period distribution of IPRNGs (2) with $a \in Z_{31}^\times$, $b \in Z_{31}^\times$ and $x_0 \in Z_{31}$. It can be seen from Fig. 2 that the periods distribute very sparsely, some exist and some do not. In the following, the period distribution rules for $a \in Z_N^\times$, $b \in Z_N^\times$ and $x_0 \in Z_N$ will be worked out analytically.

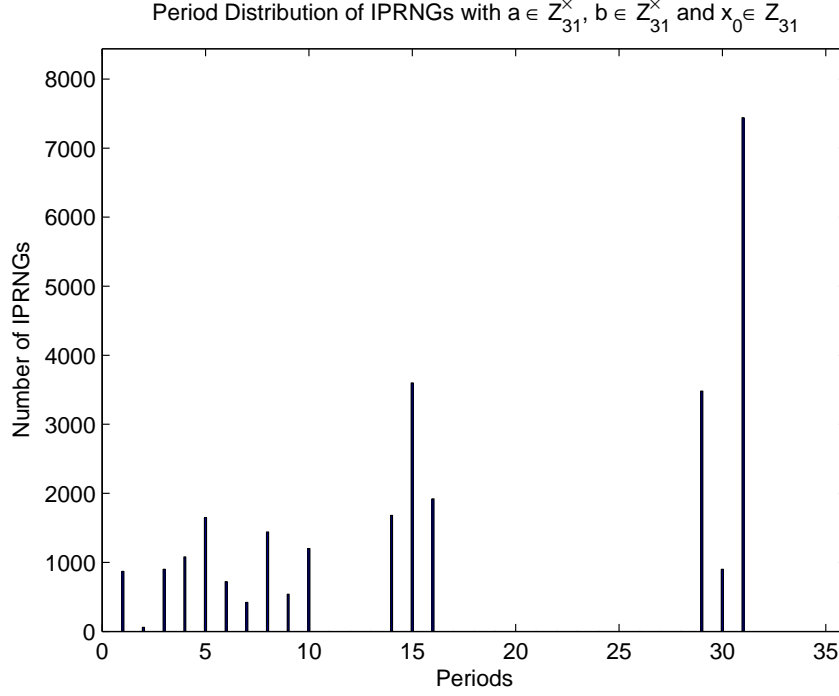


Fig. 2. Period distribution of IPRNGs with $a \in Z_{31}^\times$, $b \in Z_{31}^\times$ and $x_0 \in Z_{31}$.

In order to get the main results in the rest of this paper, we provide an important lemma in [13] which transforms the sequence generated by IPRNGs to 2-dimensional LFSR sequences.

Lemma 1: [13]. Let a, b and x_0 are in Z_N . Define the LFSR

$$y_{n+2} = by_{n+1} + ay_n, \quad (3)$$

for all $n \geq 0$, where $y_0 = 1$, $y_1 = x_0$. Then if $m \geq 0$ is an integer such that $y_n \in Z_{p^e}^\times$ for all $0 \leq n \leq m$, then $x_n = y_{n+1}y_n^{-1}$ for all $0 \leq n \leq m$. Moreover, m is the smallest positive integer satisfying $x_m = 0$ if and only if $m+1$ is the smallest integer satisfying $y_{m+1} = 0$.

Let $f(t) = t^2 - bt - a$ be the characteristic polynomial of LFSR (3). If $f(t)$ has a root with multiplicity 2, i.e., $f(t) = (t - \alpha)^2$, then $a = -\alpha^2$ and $b = 2\alpha$. It follows from (3) that

$$y_{n+2} = 2\alpha y_{n+1} - \alpha^2 y_n. \quad (4)$$

By simple calculation, we can get the general term of (4)

$$y_n = \alpha^n(n(\alpha^{-1}x_0 - 1) + 1). \quad (5)$$

If $f(t)$ has two distinct roots with multiplicity 1, i.e., $f(t) = (t - \alpha)(t - \beta)$ and $\alpha \neq \beta$, then $a = -\alpha\beta$ and $b = \alpha + \beta$. It follows from (3) that

$$y_{n+2} = (\alpha + \beta)y_{n+1} - \alpha\beta y_n. \quad (6)$$

By simple calculation, we can get the general term of (6)

$$y_n = (\alpha - \beta)^{-1}((x_0 - \beta)\alpha^n + (\alpha - x_0)\beta^n). \quad (7)$$

It can be observed from (5) and (7) that the general terms of (3) are different when $f(t)$ has a root with multiplicity 2 and has two distinct roots with multiplicity 1. Thus, we will discuss these two cases separately.

A. $f(t)$ has a root with multiplicity 2

We suppose that α is a root of $f(t)$, i.e., $f(t) = (t - \alpha)^2$. In this case, it must holds that $\alpha \in \mathbb{Z}_N$. In fact, if $\alpha \notin \mathbb{Z}_N$, which means that $f(t)$ is irreducible in $\mathbb{Z}_N[t]$, then $f(t)$ must have two roots in $\text{GF}(N^2)$ and all roots of $f(t)$ are α and α^N , where α and α^N are in $\text{GF}(N^2)$ but not in \mathbb{Z}_N . Since $f(t)$ has a root with multiplicity 2, it must hold that $\alpha^N = \alpha$. Thus, $\alpha^{N-1} = 1$, which means that $\text{ord}(\alpha) \mid N - 1$. Therefore, $\alpha \in \mathbb{Z}_N$, which is a contradiction.

It follows from (5) that if $x_0 \neq \alpha$, then y_n must contain 0, which means that $S(x_0; a, b)$ must contain some elements in 0; Otherwise, y_n dose not contain 0, which means that $S(x_0; a, b)$ does not contain 0.

Proposition 4: Suppose $f(t)$ has a root with multiplicity 2 in \mathbb{Z}_N . If $x_0 \neq \alpha$, then $L(x_0; a, b) = N - 1$ and there are $(N - 1)^2$ IPRNGs of period $N - 1$.

Proof: Period analysis.

Since $x_0 \neq \alpha$, it is valid that y_n must contain 0. Thus, $L(x_0; a, b) = L(b; a, b)$. When $x_0 = 2\alpha$, it follows from (5) that $y_n = (n + 1)\alpha^n$. Thus, $n = N - 1$ is the smallest integer such that $y_n = 0$. By lemma 1, we have $N - 2$ is the smallest integer such that $x_{N-2} = 0$. Thus, $x_{N-1} = b$, which means that $L(b; a, b) = N - 1$.

Counting.

When α traverses all elements in \mathbb{Z}_N^\times , there are $N - 1$ choices of α . Since $f(t) = (t - \alpha)^2$, it is valid that a and b are uniquely determined by a chosen α . Also, it follows from $x_0 \neq \alpha$ that there are $N - 1$ choices of x_0 . Thus, there are $(N - 1)^2$ IPRNGs of period $N - 1$. The proof is completed. ■

Proposition 5: Suppose $f(t)$ has a root with multiplicity 2 in $\mathbb{Z}_N[t]$. If $x_0 = \alpha$, then $L(x_0; a, b) = 1$ and there are $N - 1$ IPRNGs of period 1.

Proof: Period analysis.

Since $x_0 = \alpha$, it is valid that y_n does not contain 0. It follows from (5) that $y_n = \alpha^n$. By lemma 1, we can get that $x_n = \alpha$ for all $n = 1, 2, \dots$. Thus, $L(x_0; a, b) = 1$.

Counting.

When α traverses all elements in \mathbb{Z}_N^\times , there are $N - 1$ choices of α . Since $f(t) = (t - \alpha)^2$, it is valid that a and b are uniquely determined by a chosen α . Also, it follows from $x_0 = \alpha$ that there is a unique choice of x_0 . Thus, there are $N - 1$ IPRNGs of period 1. The proof is completed. ■

B. $f(t)$ has two distinct roots with multiplicity 1

It follows from (7) that $y_n = 0$ if and only if

$$(x_0 - \alpha)(x_0 - \beta)^{-1} = (\alpha\beta^{-1})^n. \quad (8)$$

For presentation convenience, we denote set $\Omega = \{\alpha\beta^{-1}, (\alpha\beta^{-1})^2, \dots, (\alpha\beta^{-1})^{\text{ord}(\alpha\beta^{-1})-1}\}$.

If $(x_0 - \alpha)(x_0 - \beta)^{-1} \in \Omega$, there exists $1 \leq n \leq p - 1$ such that (8) holds, thus, $S(x_0; a, b)$ must contains some elements in 0; if $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$, there does not exist any n such that (10) holds, thus, $S(x_0; a, b)$ does not contain any element in 0.

On the other hand, if either $x_0 - \alpha = 0$ or $x_0 - \beta = 0$, then $y_n \neq 0$ for all $n = 1, 2, \dots$, which means that $S(x_0; a, b)$ does not contain any element in 0.

In the following, we will provide three lemmas which are necessary for our analysis.

Lemma 2: Suppose $a \in Z_N^\times$, $b \in Z_N^\times$. Then, if α, β are two distinct roots of $f(t)$, then $\text{ord}(\alpha\beta^{-1}) > 2$.

Proof: Since $b \in Z_N^\times$ and $b = \alpha + \beta$, it holds that $\alpha + \beta \neq 0$. Combining $\alpha - \beta \neq 0$, we have $\alpha\beta^{-1} - \alpha^{-1}\beta \neq 0$, which means that $\alpha\beta^{-1} \neq \alpha^{-1}\beta$. If $\text{ord}(\alpha\beta^{-1}) = 1$, then it must hold that $\alpha\beta^{-1} = 1$ and $\alpha\beta^{-1} = 1$, which contradicts to $\alpha\beta^{-1} \neq \alpha^{-1}\beta$. If $\text{ord}(\alpha\beta^{-1}) = 2$, then it follows from $\varphi(2) = 1$. Thus, $\alpha\beta^{-1} = \alpha^{-1}\beta$, which is a contradiction. The proof is completed. ■

Lemma 3: Suppose $a \in Z_N^\times$, $b \in Z_N^\times$. If α, β are two distinct roots of $f(t)$, then $\alpha\beta^{-1}$ and $\alpha^{-1}\beta$ are two roots of $g(t) = t^2 + (a^{-1}b^2 + 2)t + 1$.

Proof: Since α, β are two distinct roots of $f(t)$, it is valid that $a = -\alpha\beta$ and $b = \alpha + \beta$. Then, it is easy to verify that $\alpha\beta^{-1}$ and $\alpha^{-1}\beta$ are roots of $g(t)$. The proof is completed. ■

Lemma 4: Suppose $a \in Z_N^\times$, $b \in Z_N^\times$. If α, β are two distinct roots of $f(t)$, then $a^{-1}b^2$ is uniquely determined by $\alpha\beta^{-1}$.

Proof: Since $\alpha\beta^{-1}$ and $\alpha^{-1}\beta$ are roots of $g(t)$, it holds that $a^{-1}b^2 + 2 = \alpha\beta^{-1} + \alpha^{-1}\beta$.

If $a^{-1}b^2$ is not uniquely determined by $\alpha\beta^{-1}$ or $\alpha^{-1}\beta$, then there exist $\alpha_1\beta_1^{-1}$ and $\alpha_2\beta_2^{-1}$ with $\alpha_1\beta_1^{-1} \neq \alpha_2\beta_2^{-1}$ and $\alpha_1\beta_1^{-1} \neq (\alpha_2\beta_2^{-1})^{-1}$, such that $\alpha_1\beta_1^{-1} + \alpha_1^{-1}\beta_1 = \alpha_2\beta_2^{-1} + \alpha_2^{-1}\beta_2$. Let $\gamma_1 = \alpha_1\beta_1^{-1}$ and $\gamma_2 = \alpha_2\beta_2^{-1}$, then we have $\gamma_1 \neq \gamma_2^{-1}$ and $\gamma_1 \neq \gamma_2$. However, by simple calculation, we have $\gamma_1 + \gamma_1^{-1} = \gamma_2 + \gamma_2^{-1}$ if and only if $(\gamma_1\gamma_2 - 1)(\gamma_1 - \gamma_2) = 0$, which means that either $\gamma_1\gamma_2 = 1$ or $\gamma_1 = \gamma_2$. These are the contradictions. The proof is completed. ■

When $f(t)$ has a root with multiplicity 2, its roots are in Z_N . However, when $f(t)$ has two distinct roots with multiplicity 1, its roots may be in $\text{GF}(N^2)$ but not in Z_N . Therefore, it is nature to consider the the following two cases separately: 1) α and β are in Z_N ; 2) α and β are in $\text{GF}(N^2)$ but not in Z_N .

1) α and β are in Z_N :

Proposition 6: Suppose $f(t)$ has two distinct roots with multiplicity 1 in Z_N . If $(x_0 - \alpha)(x_0 - \beta) \neq 0$ and $(x_0 - \alpha)(x_0 - \beta)^{-1} \in \Omega$, then $L(x_0; a, b)$ traverses the set $\{k - 1 : k > 2, k \mid N - 1\}$. For each k , there are $(k - 1)(N - 1)\frac{\varphi(k)}{2}$ IPRNGs of period $k - 1$.

Proof: Period analysis.

If $(x_0 - \alpha)(x_0 - \beta)^{-1} \in \Omega$, then $S(x_0; a, b)$ must contain 0. Thus, $L(x_0; a, b) = L(b; a, b)$. Then, we consider the case that $x_0 = b$, which means that $x_0 = \alpha + \beta$. By (7), we have $y_n = 0$ if and only if $(\alpha\beta^{-1})^{n+1} = 1$. Thus, $n = \text{ord}(\alpha\beta^{-1}) - 1$ is the smallest integer such that $y_n = 0$. By Lemma 1, we have $x_{n-1} = 0$, thus, $x_n = b$, which means that $L(x_0; a, b) = \text{ord}(\alpha\beta^{-1}) - 1$.

Since $\alpha\beta^{-1} \in \mathbb{Z}_N^\times$, it holds that $\text{ord}(\alpha\beta^{-1}) \mid N - 1$ and $\text{ord}(\alpha\beta^{-1}) > 2$. Hence, $L(x_0; a, b)$ traverses the set $\{k - 1 : k > 2, k \mid p - 1\}$.

Counting.

For $L(x_0; a, b) = k - 1$, there are $k - 1$ x_0 's such that $(x_0 - \alpha)(x_0 - \beta)^{-1} \in \Omega$. Thus, there are $k - 1$ choices of x_0 .

Since $\alpha\beta^{-1}$ and $\alpha^{-1}\beta$ are roots of $g(t)$, it holds that $a^{-1}b^2 + 2 = \alpha\beta^{-1} + \alpha^{-1}\beta$. Thus, $a = b^2(\alpha\beta^{-1} + \alpha^{-1}\beta - 2)$. By Lemma 4, we have $a^{-1}b^2$ is uniquely determined by $\alpha\beta^{-1}$. Thus, when $\text{ord}(\alpha\beta^{-1}) = k$, there are $\frac{\varphi(k)}{2}$ different $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$'s. Thus, there are $\frac{\varphi(k)}{2}$ choices of $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$.

As a result of $\text{ord}(\alpha\beta^{-1}) > 2$, we have $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$ is a unit. The number of choices of b is $N - 1$. Once b and $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$ are chosen, a is uniquely determined. Hence, for each k , there are $(k - 1)(N - 1)\frac{\varphi(k)}{2}$ IPRNGs of period $k - 1$. The proof is completed. ■

Proposition 7: Suppose $f(t)$ has two distinct roots with multiplicity 1 in \mathbb{Z}_N . If $(x_0 - \alpha)(x_0 - \beta) \neq 0$ and $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$, then $L(x_0; a, b)$ traverses the set $\{k : 2 < k < N - 1, k \mid N - 1\}$. For each k , there are $(N - (k - 1))(N - 1)\frac{\varphi(k)}{2}$ IPRNGs of period $k - 1$.

Proof: Period analysis.

If $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$, then $S(x_0; a, b)$ does not contain 0. It follows from Lemma 1 and (7) that $x_n = x_0$ if and only if

$$(x_0 - \alpha)(x_0 - \beta)\alpha^n = (x_0 - \alpha)(x_0 - \beta)\beta^n. \quad (9)$$

Since $(x_0 - \alpha)(x_0 - \beta) \neq 0$, (9) is equivalent to $(\alpha\beta^{-1})^n = 1$. Thus, $L(x_0; a, b) = \text{ord}(\alpha\beta^{-1})$.

By lemma 2, we have $\text{ord}(\alpha\beta^{-1}) > 2$. On the other hand, since $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$, it must hold that $\alpha\beta^{-1}$ is not a primitive element in \mathbb{Z}_N , which means that $\text{ord}(\alpha\beta^{-1}) \neq N - 1$. Hence, $L(x_0; a, b)$ traverses the set $\{k : 2 < k < N - 1, k \mid N - 1\}$.

Counting.

For $L(x_0; a, b) = k$, there are $N - (k - 1)$ x_0 's such that $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$. Thus, there are $N - (k - 1)$ choices of x_0 .

Since $\alpha\beta^{-1}$ and $\alpha^{-1}\beta$ are roots of $g(t)$, it holds that $a^{-1}b^2 + 2 = \alpha\beta^{-1} + \alpha^{-1}\beta$. Thus, $a = b^2(\alpha\beta^{-1} + \alpha^{-1}\beta - 2)$. By Lemma 4, we have $a^{-1}b^2$ is uniquely determined by $\alpha\beta^{-1}$. Thus, when $\text{ord}(\alpha\beta^{-1}) = k$, there are $\frac{\varphi(k)}{2}$ different $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$'s. Thus, there are $\frac{\varphi(k)}{2}$ choices of $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$.

As a result of $\text{ord}(\alpha\beta^{-1}) > 2$, we have $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$ is a unit. The number of choices of b is $N - 1$. Once b and $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$ are chosen, a is uniquely determined. Hence, for each k , there are $(N - (k - 1))(N - 1)\frac{\varphi(k)}{2}$ IPRNGs of period k . The proof is completed. ■

Proposition 8: Suppose $f(t)$ has two distinct roots with multiplicity 1 in \mathbb{Z}_N . If $(x_0 - \alpha)(x_0 - \beta) = 0$, then $L(x_0; a, b) = 1$ and there are $(N - 3)(N - 1)$ IPRNGs of period k .

Proof: Period analysis.

If $(x_0 - \alpha)(x_0 - \beta) = 0$, then $y_n = x_0^n$. Thus, $x_n = x_0$ for all $n = 1, 2, \dots$, which means that $L(x_0; a, b) = 1$.

Counting.

For $L(x_0; a, b) = 1$, α, β traverses all suitable elements in \mathbb{Z}_N^\times , i.e. both $\alpha - \beta$ and $\alpha + \beta$ are units, there are $\frac{(N-3)(N-1)}{2}$ pairs of α, β . Once α, β are chosen, there are 2 choices of x_0 . Thus, there are $(N - 3)(N - 1)$ IPRNGs of period 1. The proof is completed. ■

2) α and β are in $\text{GF}(N^2)$ but not in Z_N : In this case, it must hold that $(x_0 - \alpha)(x_0 - \beta) \neq 0$. Then, we have the following results on the period distribution of IPRNGs for this case.

Proposition 9: Suppose $f(t)$ has two distinct roots with multiplicity 1 in $\text{GF}(N^2)$ but not in Z_N . If $(x_0 - \alpha)(x_0 - \beta)^{-1} \in \Omega$, then $L(x_0; a, b)$ traverses the set $\{k - 1 : k > 2, k \mid N + 1\}$. For each k , there are $(k - 1)(N - 1)\frac{\varphi(k)}{2}$ IPRNGs of period $k - 1$.

Proof: Period analysis.

If $(x_0 - \alpha)(x_0 - \beta)^{-1} \in \Omega$, then $S(x_0; a, b)$ must contain 0. Thus, $L(x_0; a, b) = L(b; a, b)$. Then, we consider the case that $x_0 = b$, which means that $x_0 = \alpha + \beta$. By (7), we have $y_n = 0$ if and only if $(\alpha\beta^{-1})^{n+1} = 1$. Thus, $n = \text{ord}(\alpha\beta^{-1}) - 1$ is the smallest integer such that $y_n = 0$. By Lemma 1, we have $x_{n-1} = 0$, thus, $x_n = b$, which means that $L(x_0; a, b) = \text{ord}(\alpha\beta^{-1}) - 1$.

By lemma 2, we have $\text{ord}(\alpha\beta^{-1}) > 2$. Since $\alpha\beta^{-1} \in \text{GF}(N^2)$, it holds that $\text{ord}(\alpha\beta^{-1}) \mid N^2 - 1$. Notice that α and β are not in Z_N and $\alpha \neq \beta$, it is valid that $\alpha\beta^{-1} \notin Z_N$. Since $Z_N \subseteq \text{GF}(N^2)$, it is valid that all units in Z_N are contained in $\text{GF}(N^2)$, which means that $\text{ord}(\alpha\beta^{-1}) \nmid N - 1$. Thus, $\text{ord}(\alpha\beta^{-1}) \mid N + 1$. Hence, $L(x_0; a, b)$ traverses the set $\{k - 1 : k > 2, k \mid N + 1\}$.

Counting.

For $L(x_0; a, b) = k - 1$, there are $k - 1$ x_0 's such that $(x_0 - \alpha)(x_0 - \beta)^{-1} \in \Omega$. Thus, there are $k - 1$ choices of x_0 .

Since $\alpha\beta^{-1}$ and $\alpha^{-1}\beta$ are roots of $g(t)$, it holds that $a^{-1}b^2 + 2 = \alpha\beta^{-1} + \alpha^{-1}\beta$. Thus, $a = b^2(\alpha\beta^{-1} + \alpha^{-1}\beta - 2)$. By Lemma 4, we have $a^{-1}b^2$ is uniquely determined by $\alpha\beta^{-1}$. Thus, when $\text{ord}(\alpha\beta^{-1}) = k$, there are $\frac{\varphi(k)}{2}$ different $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$'s. Hence, there are $\frac{\varphi(k)}{2}$ choices of $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$.

As a result of $\text{ord}(\alpha\beta^{-1}) > 2$, we have $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$ is a unit. The number of choices of b is $N - 1$. Once b and $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$ are chosen, a is uniquely determined. Hence, for each k , there are $(k - 1)(N - 1)\frac{\varphi(k)}{2}$ IPRNGs of period $k - 1$. The proof is completed. ■

Proposition 10: Suppose $f(t)$ has two distinct roots with multiplicity 1 in $\text{GF}(N^2)$ but not in Z_N . If $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$, then $L(x_0; a, b)$ traverses the set $\{k : 2 < k < N + 1, k \mid N + 1\}$. For each k , there are $(N - (k - 1))(N - 1)\frac{\varphi(k)}{2}$ IPRNGs of period k .

Proof: Period analysis.

If $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$, then $S(x_0; a, b)$ does not contain 0. It follows from Lemma 1 and (7) that $x_n = x_0$ if and only if

$$(x_0 - \alpha)(x_0 - \beta)\alpha^n = (x_0 - \alpha)(x_0 - \beta)\beta^n. \quad (10)$$

Since $(x_0 - \alpha)(x_0 - \beta) \neq 0$, (10) is equivalent to $(\alpha\beta^{-1})^n = 1$. Thus, $L(x_0; a, b) = \text{ord}(\alpha\beta^{-1})$.

By lemma 2, we have $\text{ord}(\alpha\beta^{-1}) > 2$. Since $\alpha\beta^{-1} \in \text{GF}(N^2)$, it holds that $\text{ord}(\alpha\beta^{-1}) \mid N^2 - 1$. Notice that α and β are not in Z_N and $\alpha \neq \beta$, it is valid that $\alpha\beta^{-1} \notin Z_N$. Since $Z_N \subseteq \text{GF}(N^2)$, it is valid that all units in Z_N are contained in $\text{GF}(N^2)$, which means that $\text{ord}(\alpha\beta^{-1}) \nmid N - 1$. Thus, $\text{ord}(\alpha\beta^{-1}) \mid N + 1$.

On the other hand, since $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$, it must hold that $\alpha\beta^{-1}$ is not a primitive element in $\text{GF}(N^2)$, which means that $\text{ord}(\alpha\beta^{-1}) \neq N + 1$. Hence, $L(x_0; a, b)$ traverses the set $\{k : 2 < k < N + 1, k \mid N + 1\}$.

Counting.

For $L(x_0; a, b) = k$, there are $N - (k - 1)$ x_0 's such that $(x_0 - \alpha)(x_0 - \beta)^{-1} \notin \Omega$. Thus, there are $N - (k - 1)$ choices of x_0 .

TABLE III
PERIOD DISTRIBUTION OF IPRNGs WITH $a \in \mathbb{Z}_N^\times$, $b \in \mathbb{Z}_N^\times$ AND $x_0 \in \mathbb{Z}_N$.

Periods	Number of IPRNGs
1	$(N-2)(N-1)$
$N-1$	$(N-1)^2$
$\{k-1 : k > 2, k \mid N-1\}$	$(k-1)(N-1)\frac{\varphi(k)}{2}$
$\{k-1 : k > 2, k \mid N+1\}$	$(k-1)(N-1)\frac{\varphi(k)}{2}$
$\{k : 2 < k < N-1, k \mid N-1\}$	$(N-(k-1))(N-1)\frac{\varphi(k)}{2}$
$\{k : 2 < k < N+1, k \mid N+1\}$	$(N-(k-1))(N-1)\frac{\varphi(k)}{2}$

Since $\alpha\beta^{-1}$ and $\alpha^{-1}\beta$ are roots of $g(t)$, it holds that $a^{-1}b^2 + 2 = \alpha\beta^{-1} + \alpha^{-1}\beta$. Thus, $a = b^2(\alpha\beta^{-1} + \alpha^{-1}\beta - 2)$. By Lemma 4, we have $a^{-1}b^2$ is uniquely determined by $\alpha\beta^{-1}$. Thus, when $\text{ord}(\alpha\beta^{-1}) = k$, there are $\frac{\varphi(k)}{2}$ different $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$'s. Thus, there are $\frac{\varphi(k)}{2}$ choices of $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$.

As a result of $\text{ord}(\alpha\beta^{-1}) > 2$, we have $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$ is a unit. The number of choices of b is $N-1$. Once b and $\alpha\beta^{-1} + \alpha^{-1}\beta - 2$ are chosen, a is uniquely determined. Hence, for each k , there are $(N-(k-1))(N-1)\frac{\varphi(k)}{2}$ IPRNGs of period k . The proof is completed. ■

Now, we summarize the results in the following theorem.

Theorem 2: For IPRNGs with $a \in \mathbb{Z}_N^\times$, $b \in \mathbb{Z}_N^\times$ and $x_0 \in \mathbb{Z}_N$, the possible periods and the number of each special period are given in Table III.

Remark 2: It should be mentioned that $N > 3$ is an important condition in Theorem 3, because of some periods require $k > 2, k \mid N-1$, which implies that $N > 3$.

Example 2: The following example is given to compare experimental and the theoretical results. A computer program has been written to exhaust all possible IPRNGs with $a \in \mathbb{Z}_{31}^\times$ and $b \in \mathbb{Z}_{31}^\times$ and $x_0 \in \mathbb{Z}_{31}$ to find the period by brute force, the results are shown in Fig. 2.

Table IV lists the complete result we have obtained. It provides the period distribution of the IPRNGs. As it is shown in Fig. 2 and Table IV, the theoretical and experimental results fit well. The maximal period is 31 while the minimal period is 1. The analysis process also indicates how to choose the parameters and the initial values such that the IPRNGs fit specific periods.

V. CONCLUSION

The period distribution of the IPRNGs over $(\mathbb{Z}_N, +, \times)$ for prime $N > 3$ has been analyzed. The period distribution of IPRNGs is obtained by the generating function method and the finite field theory. The analysis process also indicates how to choose the parameters and the initial values such that the IPRNGs fit specific periods. The analysis results show that the period distribution is poor if N is not chosen properly and there are many small periods.

TABLE IV
PERIOD DISTRIBUTION OF IPRNGs WITH $a \in \mathbb{Z}_{31}^\times$, $b \in \mathbb{Z}_{31}^\times$ AND $x_0 \in \mathbb{Z}_{31}$

Periods	1	2	3	4	5	6	7	8
Number of IPRNGs	870	60	900	1080	1650	720	420	1440
Periods	9	10	14	15	16	29	30	31
Number of IPRNGs	540	1200	1680	3600	1920	3480	900	7440

A feasible way to resolve the open problem proposed by Solé *et al.* in [14] is to analyze the period distribution of the sequence generated by IPRNGs over Galois rings. However, the period distribution of IPRNG sequences varies substantially as N changes, when N is a prime, $(\mathbb{Z}_N, +, \times)$ is a finite field; when N is a power of prime, i.e., $N = p^e$, $(\mathbb{Z}_N, +, \times)$ is a Galois ring. The structure of $(\mathbb{Z}_{p^e}, +, \times)$ is more complicated than that of $(\mathbb{Z}_N, +, \times)$, because of $(\mathbb{Z}_{p^e}, +, \times)$ contains many zero divisors but $(\mathbb{Z}_N, +, \times)$ does not, this difference makes the fact that the analysis in Galois rings is more complicated than that in finite fields, which is challenging and deserves intensive study. Another important problem is to characterize the security properties of the IPRNGs. These topics are interesting and need further research.

ACKNOWLEDGEMENTS

This work was partially supported by the National Natural Science Foundation of China under Grant 60974132, the Natural Science Foundation Project of CQ CSTC2011BA6026 and the Scientific & Technological Research Projects of CQ KJ110424.

REFERENCES

- [1] T. Stojanovski, L. Kocarev, Chaos-based random number generators-part I: analysis, IEEE Trans. Circuits Syst. I, Fundam. Theory Appl. 48(3)(2009) 281-299.
- [2] J. Eichenauer, J. Lehn, A non-linear congruential pseudorandom number generator, Stat. Pap. 27(1)(1986) 315-326.
- [3] R.S. Katti, R.G. Kavasseriand, V. Sai, Pseudorandom bit generation using coupled congruential generators, IEEE Trans. Circuits Syst. II, Exp. Briefs 57(3)(2010) 203-207.
- [4] T. Addabbo, M. Alioto, A. Fort, A. Pasini, S. Rocchi, V. Vignoli, A class of maximum-period nonlinear congruential generators derived from the Rényi chaotic map, IEEE Trans. Circuits Syst. I: Reg. Papers 54(4)(2007) 816-828.
- [5] G.R. Chen, Y.B. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Soliton. Fract. 21(3)(2004) 749-761.
- [6] L. Kocarev, G. Jakimoski, Pseudorandom bits generated by chaotic maps, IEEE Trans. Circuits Syst. I, Fundam. Theory Appl. 50(1)(2003) 123-126.
- [7] L. Kocarev, J. Makraduli and P. Amato, Public-Key Encryption Based on Chebyshev Polynomials, Circ. Syst. Signal Pr. 24(5)(2005) 497-517.
- [8] R. Kuehnel, J. Theiler, Y. Wang, Parallel random number generators for sequences uniformly distributed over any range of integers, IEEE Trans. Circuits Syst. I, Reg. Papers 53(7)(2006) 1496-1505.
- [9] F. Chen, X.F. Liao, T. Xiang, H.Y. Zheng, Security analysis of the public key algorithm based on Chebyshev polynomials over the integer ring \mathbb{Z}_N , Inform. Sciences 181(22)(2011) 5110-5118.

- [10] X.F. Liao, F. Chen, K.W. Wong, On the security of public-key algorithms based on chebyshev polynomials over the finite field Z_N , IEEE Trans. Comput. 59(10)(2010) 1392-1401.
- [11] F. Chen, K.W. Wong, X.F. Liao, T. Xiang, Period distribution of generalized discrete Arnold cat map for $N = p^e$, IEEE Trans. Inform. Theory 58(1)(2012) 445-452.
- [12] F. Chen, X.F. Liao, K.W. Wong, Q. Han, Y. Li, Period distribution analysis of some linear maps, Commun. Nonlinear Sci. 17(10)(2012) 3848-3856.
- [13] W.S. Chou, The period lengths of inversive pseudorandom vector generations, Finite Fields Th. App. 1(1)(1995) 126-132.
- [14] P. Solé, D. Zinoviev, Inversive pseudorandom numbers over Galois rings, Eur. J. of Combin. 30(2)(2009) 458-467.
- [15] J. Gutierrez, H. Niederreiter, I.E. Shparlinski, On the Multidimensional Distribution of Inversive Congruential Pseudorandom Numbers in Parts of the Period, Monatsh. Math. 129(1)(2000) 31-36.
- [16] H. Niederreiter, I.E. Shparlinski, On the distribution of inversive congruential pseudorandom numbers in parts of the period, Math. comput. 70 (236)(2000) 1569-1574.
- [17] R.A. Rueppel, Analysis and Design of Stream Ciphers, New York, NY: Springer-Verlag, 1986.
- [18] R. Lidl and H. Niederreiter, Finite Fields, Vol. 20, Encyclopedia of Mathematics and Its Applications, Amsterdam, The Netherlands: Addison-Wesley, 1983.